IN THE UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF MISSOURI
WESTERN DIVISION

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
v.	)	Criminal Action No.
	)	07-00006-01-CR-W-SOW
GREGORY SAGE,	)	
	)	
Defendant.	)	

REPORT AND RECOMMENDATION TO DENY DEFENDANT'S MOTION TO SUPPRESS EVIDENCE

Before the court is a motion to suppress evidence filed by defendant Gregory Sage on the ground that the information seized was not described with particularity in the warrant, and the warrant was illegally executed. I find that regardless of whether the particularly requirement of the Fourth Amendment was met with regard to the items to be seized, the good-faith exception to the exclusionary rule applies. Therefore, defendant's motion to suppress should be denied.

I. BACKGROUND

In August 2006, police learned from a minor that he had engaged in sexual acts with the defendant on two separate occasions. The minor stated that he had communicated with defendant by cell phone text messages and through instant messages on the computer. Police obtained a search warrant authorizing the seizure of "any and all" media and data stored in defendant's computer or cell phone. Police seized defendant's

computer and searched specifically for evidence of contacts between defendant and the victim as well as for child pornography. They did indeed find child pornography on defendant's computer.

On January 4, 2007, an indictment was returned charging defendant with four counts of receipt of child pornography over the internet, in violation of 18 U.S.C. § 2252(a)(2), and one count of possession of child pornography, in violation of 18 U.S.C. § 2252(a)(4). Defendant filed a motion to suppress evidence on February 12, 2007 (document number 23). That motion was held in abeyance pending the determination of defendant's mental competency. On February 28, 2007, the government filed a response in opposition to defendant's motion (document number 28).

On September 17, 2007, I held an evidentiary hearing on defendant's motion to suppress evidence. The government appeared by Assistant United States Attorney Katharine Fincham. The defendant was present, represented by J.R. Hobbs. The following witnesses testified:

1. Detective Rachel Casady, Lee's Summit, Missouri, Police Department
2. Detective Mark Phillips, Lee's Summit, Missouri, Police Department
3. Richard Gatewood, Forensics Examiner with Heart of America Regional Computer Forensic Lab

In addition, the following exhibits were admitted:

P. Ex. 1 Affidavit for search warrant dated September 1, 2006

P. Ex. 2 Search warrant dated September 1, 2006

P. Ex. 3 Photograph of XY magazine showing a boy clothed only in boxer shorts on the cover

P. Ex. 4 Photograph of police radio located on defendant's bedroom dresser

P. Ex. 5 Photograph of police radios in defendant's bedroom

P. Ex. 6 Photograph of a camera bag on a chair in defendant's living room

P. Ex. 7 Photograph of police scanner located in defendant's bedroom closet

P. Ex. 8 Search warrant return

P. Ex. 9 Request for Service, Heart of America Regional Computer Forensic Lab, dated September 5, 2006

P. Ex. 10 Narrative Supplement prepared by Detective Phillips

P. Ex. 11 After-Action Police Report completed by Detective Phillips

P. Ex. 12 Curriculum Vitae for Richard Gatewood

II. EVIDENCE

On the basis of the evidence presented at the suppression hearing, I submit the following findings of fact:

1. In August 2007, police learned from a minor, D.C., that he had had sexual contact with defendant Gregory Sage in exchange for money on two separate occasions (P. Ex. 1). D.C. stated that he had had sexual contact with defendant in defendant's car on one occasion and in defendant's residence on another (P. Ex. 1). He and defendant had met online and had communicated by cell

telephone text messages and through instant messages on the computer (P. Ex. 1). D.C. did not tell the police that defendant ever displayed child pornography (Tr. at 34, 36). D.C. did not indicate that there were other alleged victims who had had sexual contact with defendant (Tr. at 34-35).

2. On September 1, 2006, a search warrant was issued which authorized the search of the following things, reported to be located within defendant's residence:

> 1. Any and all computer component systems (CPU's), specifically, but not limited to, a laptop computer, last seen on the glass coffee table in the living room area.
> 2. Gray-colored Nextel cellular flip phone.

(P. Ex. 1).

3. The warrant authorized police to seize the following items:

> 1. Any and all electronic and internal media stored within the above computer electronic items, together with all storage devices, internal or external to the computer or computer system.
> 2. Any and all electronic data stored within the above-described computer (CPU) and cell phone. The search should include all logs of incoming numbers, outgoing numbers dialed, phonebook (contact numbers), voice messages, and other recordings, and images stored within the phone as well as the subscriber identity module (SIM) card.

(P. Ex. 1).

4. When preparing the application for search warrant, Detective Casady obtained a sample search warrant from Detective Lyles (Tr. at 8). After she completed the application in this

case, Detective Casady had the paperwork reviewed by Detective Lyles, Sgt. Black, and Detective Mark Phillips (Tr. at 8). Detective Phillips suggested a few changes to the narrative portion, and Detective Casady made those changes (Tr. at 8). For example, he advised her to be more specific about the laptop computer, its location, what it was used for, and the communication between the victim and the defendant in this case (Tr. at 9).

5. The probable cause portion of the search warrant application reads as follows:

> On 8-21-06, sixteen-year-old "D.C." reported to the Lee's Summit Police Department that he had sexual contact with a twenty-four year old male named "Greg Sage" on 8-21-06 at 0100 hours. On 8-30-06, D.C. stated to Detective Rachel Casady that Greg Sage had performed oral sex on D.C. on 8-13-06 while in Sage's vehicle, and D.C. had ejaculated. D.C. also stated that Greg Sage paid him $60.00 for him (Greg) to give D.C. a "blowjob." D.C. further stated that he had been picked up by Greg Sage in Sage's car on 8-21-06, and driven to Greg Sage's residence. D.C. Stated that Greg Sage performed oral sex on him, and had also engaged in anal intercourse by placing his penis inside Sage's anus on 8-21-06, and D.C. had ejaculated. D.C. stated that Greg Sage had paid him $80.00 for the sexual activity on 8-21-06.
>
> D.C. reported that he had met Greg Sage online at his MySpace.com blog account in approximately mid-July 2006. He stated that he and Greg Sage communicated "every day" via his home computer through MySpace.com and American [sic] Online Instant Messenger "chat room." D.C. stated that while at Greg Sage's house, located at 1454 SW Manor Lake Drive, Lee's Summit, Jackson County, Missouri[1], he observed

[1]During an interview with police, the victim provided a description of defendant's residence (Tr. at 6). In addition, he went with Detective Rachel Casady to defendant's residence and pointed it out (Tr. at 6).

> a laptop computer with an attached mouse on a glass coffee table in the residential living room area. D.C. reported to me that Greg Sage would tell him that he was on his home laptop computer while communicating via the Internet with him. D.C. also reported that he would receive text messages on his cellular phone from Greg Sage, that Sage would send from his Nextel cellular phone.
>
> AOL [America Online] does not archive chat room messages on their online server. However, this information is placed on the user's computer as digital information in a text format. To further the investigation or establish that the offense has been committed, this information is needed to be recovered.

(P. Ex. 1).

6. MySpace accounts normally contain pictures of people's friends and images of people's cars and other prized possessions (Tr. at 6-7, 22). A person can send messages on a MySpace account which can be viewed on the main page by everyone on that account (Tr. at 7). Multiple users can also send private messages back and forth (Tr. at 7).

7. When you pull up someone's MySpace profile page, you may send a message to that person if you are on the person's "friends" list (Tr. at 8).

8. There was no representation that defendant's MySpace profile contained images of child pornography (Tr. at 22). However, Detective Casady had attended a training course where she learned there may be a connection between sexual contact with a minor and child pornography (Tr. at 35-36).

9. Detective Casady checked the history of the Lee's Summit Police Department regarding obtaining search warrants for

computer media (Tr. at 9). She learned that approximately 15 warrants had been sought for computer media, and they all contained language similar to the application she had prepared (Tr. at 9). None of those had been challenged in court (Tr. at 9, 20-21).

10. Detective Casady did not attempt to restrict the warrant to review of text messages (Tr. at 22-24). Detective Casady did not attempt to restrict or confine the search to files commonly associated with AOL software and chat logs (Tr. at 24-25).

11. Once she had completed the application, Detective Casady met with Jackson County Prosecutor Brian Kavinsky at the Independence courthouse (Tr. at 9, 31). Mr. Kavinsky reviewed the application and affidavit and did not make any changes to them (Tr. at 10).

12. Detective Casady then met with Judge Michael Manners (Tr. at 10). Judge Manners read the affidavit/application and then signed the warrant (Tr. at 10-11). Although Judge Manners did not make any corrections to the affidavit/application, he did correct the date that appeared on the actual search warrant (Tr. at 11; P. Ex. 2). Judge Manners changed the typed date from March 31 to September 1, and then he initialed that change (Tr. at 12, 27; P. Ex. 2).

13. Once the warrant was signed, Detective Casady met with other detectives at police headquarters, went over the search warrant, provided the address where the warrant would be executed, and made sure someone had a video camera and a camera (Tr. at 12). Detective Mark Phillips was designated as the person to receive and log the items seized (Tr. at 12).

14. During execution of the search warrant, police observed in a drawer a magazine showing a boy clothed only in boxer shorts (Tr. at 13). They photographed the magazine but did not seize it because they believed it was outside the scope of the warrant since it was not listed as an item to be seized (Tr. at 13, 29).

15. Police observed a police radio on defendant's bedroom dresser; however, it was not seized because police believed it was outside the scope of the search warrant (Tr. at 13-14). The police scanner was photographed (Tr. at 14; P. Ex. 4).

16. Police observed more police radios located on one of defendant's bedroom dressers (Tr. at 14). They photographed the scanners but did not seize them because they believed the scanners were outside the scope of the search warrant (Tr. at 14; P. Ex. 5).

17. Police found a camera bag with a camera inside (Tr. at 14-15). The bag was lying on a chair in defendant's living room (Tr. at 14-15). Police photographed the camera bag but did not seize it or the camera because they believed it was outside the

scope of the search warrant (Tr. at 15; P. Ex. 6).

18. Police found a police scanner in the bedroom closet (Tr. at 15). They photographed the scanner but did not seize it because they believed it was outside the scope of the search warrant (Tr. at 15; P. Ex. 7).

19. During the search, police seized a laptop computer located on the coffee table, a CPU tower, two flash drives, some compact disks, an external hard drive, and two phones (Tr. at 16; P. Ex. 8).

20. A couple of days after these items were seized, Detective Casady completed a Request for Service form for the Heart of America Regional Computer Forensic Lab ("RCFL") (Tr. at 17; P. Ex. 9). The form requested examination for any programs containing child pornography and/or communication between the computer owner and the named victim[2] (P. Ex. 9). That form was forwarded to the RCFL along with the computer media and a copy of the search warrant but not the affidavit (Tr. at 17-18). Child pornography was included in the request because the victim had admitted that there was sexual contact between himself and the defendant on more than one occasion, and the police found the XY

[2]"I am requesting examination of the hard drive and any programs containing child pornography and/or communication between the computer owner and victim [name redacted]. This should include all saved and unsaved chat room logs, MySpace account conversations located on the computer, CPU, SanDisk flash drive, PNY flash drive, or Seagate external hard drive submitted." (Tr. at 18; P. Ex. 9).

magazine in defendant's residence (Tr. at 18-19). In addition, Detective Casady has been taught in her training that it is not uncommon to find child pornography in the possession of child predators (Tr. at 19).

21. Before RCFL will examine a computer, a "preview" must be done by the police (Tr. at 19). Detective Mark Phillips was assigned to do the preview, and Detective Casady provided him with user names, account names from defendant's MySpace account, and AOL Instant Messenger chat room screen names (Tr. at 19). Detective Phillips believed that the search warrant authorized him to look at anything that was on the defendant's computer (Tr. at 43, 55). Detective Phillips was specifically looking for child pornography and chats or other information involving the victim of this particular case and the defendant (Tr. at 44, 56).

22. The software used by Detective Phillips, FTK, organizes the computer material into groups which are tabbed; and the first tab is the graphics tab, which is the one Detective Phillips opened first (Tr. at 44). Detective Phillips looked for pictures of D.C., pictures that would possibly be on his MySpace account, or anything else he would have out on the internet (Tr. at 45).

23. Because text documents can be misidentified as image documents[3], if Detective Phillips is looking for a text document,

[3]Text documents typically end in ".txt" or ".doc", and graphics typically end in ".jpg", ".bmp", ".jpeg.", or ".wmv" (Tr. at 77). A user can camouflage an image by changing the

he would have to look everywhere (Tr. at 45).

24. When Detective Phillips first began viewing the image documents, he observed many pictures of younger males and he bookmarked[4] them for later analysis because he thought they might be pictures of additional victims (Tr. at 45-46). Detective Phillips also observed child pornography (Tr. at 46). He believed the child pornography was evidence in this case because child pornography and child enticement "go hand in hand" (Tr. at 47). Detective Phillips did not alter his search plan after he found the child pornography; he had originally intended to go through the entire computer (Tr. at 47, 67, 79, 81).

25. Detective Phillips learned that defendant was a freelance photographer with a school district and took a lot of pictures of kids at sporting events; therefore, he stopped bookmarking pictures of kids that were not pornographic (Tr. at 47-48).

26. Detective Phillips bookmarked pictures of automobiles in case any of them were identified as the defendant's automobile or one belonging to any other victim (Tr. at 48).

---

extension to a text extension, like ".txt" (Tr. at 77). Then the picture would look like a text document, or vice versa (Tr. at 77).

[4]All of the items bookmarked are saved onto a disk so that the investigator can look at those items and determine whether they are important to the investigation (Tr. at 73).

27. Detective Phillips reviewed evidence of a file sharing program called Limewire (Tr. at 49). Limewire is used very frequently in the transfer of child pornography from one computer to another (Tr. at 49). Detective Phillips found movie files of child pornography on defendant's computer which had been downloaded through Limewire, and he bookmarked some of those (Tr. at 49-50). He does not know whether he bookmarked them all because he stopped reviewing them due to the large quantity (Tr. at 50).

28. Detective Phillips conducted string searches with relevant words he had obtained from Detective Casady (Tr. at 50, 59). Those included screen names, information that was used in speaking with the victim, e-mail i.d.'s, etc. (Tr. at 50). None of those buzz words were designed to uncover child pornography (Tr. at 51; P. Ex. 10, p.3-4). The string searches would search through text documents and not images (Tr. at 74).

29. Once Detective Phillips was done with his preview, he completed a Narrative Supplement which summarized the work he did and some of his findings (Tr. at 50; P. Ex. 10). Detective Phillips then requested that RCFL complete the analysis of the computer and look for additional evidence because Detective Phillips had not found a lot of text messaging between defendant and D.C. (Tr. at 52). This was done in an after-action police report showing what he did and did not find in his analysis, and

what analysis he specifically wanted from RCFL (Tr. at 52; P. Ex. 11). The request included a notation that the case was going to the "Feds" and "is somewhat of a political hotbed" and requested that if possible, a rush be put on the analysis (Tr. at 65, 67; P. Ex. 11). Detective Phillips used this description of the case because defendant and his family were friends with police administration, defendant was a DJ with a popular top 40 radio station, and he was a freelance photographer with schools and the schools were calling in about defendant's arrest (Tr. at 65). Therefore, with all of the inquiries coming from within and outside of the police department, Detective Phillips categorized it as a political hotbed (Tr. at 65, 75).

30. Detective Casady's request for service by RCFL was not her attempt to expand the search to items containing child pornography, because she believed the search warrant already covered child pornography due to its authorizing her to seize "any and all media" located in the computer components (Tr. at 34).

31. According to Detective Phillips, if he were looking only for interactions between defendant and D.C., it would be impossible not to stumble across something else (Tr. at 68). This is because he would have to search the HTML tab, which is internet pages, and those have graphics in them (Tr. at 70). Therefore, in order to review e-mails, he would need to review

the web page tab and would run into graphics (Tr. at 70). He could substantially limit his review of graphics, although not eliminate it, by not going into the graphics tab (Tr. at 71-72, 78, 79). When he reviewed Zip files, he may run into graphics, because Zip files can be groups of text documents compressed into one file, or they can be groups of pictures compressed into one file (Tr. at 73).

32. If he were limited to searching only for text interactions and he stumbled across child pornography, he would stop the search and request an additional search warrant (Tr. at 68-69). If he were looking for pictures of defendant's car, he would need to search all of the graphics files (Tr. at 84).

33. Richard Gatewood, a forensics examiner with Heart of America Regional Computer Forensic Lab, received the request from the Lee's Summit Police Department completed by Detective Casady (Tr. at 90). He also received a copy of the search warrant (Tr. at 91). He read the search warrant to make sure it covered the service request (Tr. at 91).

34. If he was directed to look for pictures of a person's vehicle, Mr. Gatewood would go to the graphics tab of the FTK program (Tr. at 93). Once in the graphics tab, there is no way to limit the search of graphics to target vehicles (Tr. at 93).

35. There was nothing about the reference to a political hotbed that altered how Mr. Gatewood conducted his analysis (Tr.

at 93). Mr. Gatewood believed that the search warrant authorized the searches that he conducted in this case because it authorized the search and seizure of "any and all electronic media" (Tr. at 97).

III. PARTICULARITY REQUIREMENT

The Fourth Amendment states that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized". The purpose of the particularly requirement is to prevent a general exploratory rummaging through a person's belongings. Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971); United States v. Mosby, 101 F.3d 1278, 1281 (8th Cir. 1996).

To satisfy the particularly requirement of the Fourth Amendment, the warrant must be sufficiently definite to enable the searching officers to identify the property authorized to be seized. United States v. Summage, 481 F.3d 1075, 1079 (8th Cir. 2007), petition for cert. filed Sept. 6, 2007 (No. 07-6407). The degree of specificity required depends on the circumstances of the case and on the type of items involved. Id. The particularity requirement is a standard of practical accuracy rather than a hypertechnical one. Id. See also United States v. Horn, 187 F.3d 781, 788 (8th Cir. 1999); United States v. Peters, 92 F.3d 768, 769-70 (8th Cir. 1996).

In this case, the warrant authorized the search of "any and all computer component systems (CPU's), specifically, but not limited to, a laptop computer, last seen on the glass coffee table in the living room area" and a "gray-colored Nextel cellular flip phone". The police actually seized a laptop computer located on the coffee table, a CPU tower, two flash drives, some compact disks, an external hard drive, and two phones.

> The requirement of particularity must be assessed in terms of practicality. As a practical matter, it is frequently difficult, and often times more intrusive to an individual's privacy, to perform an on-site review of certain items. United States v. Hill, 459 F.3d 966, 974-75 (9th Cir. 2006) (recognizing that an on-site search of a computer "could take many hours and perhaps days" and "would not only impose a significant and unjustified burden on police resources, it would also make the search more intrusive"); United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999) ("As a practical matter, the seizure and subsequent off-premises search of the computer and all available disks was about the narrowest definable search and seizure reasonably likely to obtain the images."); Horn, 187 F.3d at 788 (concluding that the officers could not practically view all the videos at the search site). An off-site analysis of the relevant materials is therefore often necessary.
>
> Because no indication was given regarding the nature of the format in which the sought-for video and photographs were created or stored, it was necessary to search a broad array of items for the relevant materials, the on-site search of which could take a significant amount of time. Given these circumstances and the practical concerns associated therewith, we conclude that the warrant was neither over-broad nor lacking in particularity.

United States v. Summage, 481 F.3d at 1079-80.

Here, the warrant authorized police to search the computer and the cell phone for media and data. Police went to

defendant's residence, and seized only the computer equipment authorized by the warrant and two cell phones. Because it would be impractical and overly intrusive to defendant's privacy for police to remain in the residence for days in order to search through the media and data in the computer and phones, the police were justified in removing those items from defendant's residence.

The crux of defendant's argument, however, is not so much the removal of those items from his residence, but the officers' looking at everything stored in his computer, including images, when there was no allegation by the victim that any images (such as pornography) were used or discussed during the sex crimes that were being investigated. Because the affidavit does not even mention child pornography, a strong argument can be made that the affidavit does not establish probable cause to search for child pornography. It is clear that the detectives did not merely "run across" the child pornography while searching for evidence of contacts between defendant and D.C. Indeed, Detective Casady's Request for Service to the Heart of America Regional Computer Forensic Lab requested examination for any program containing not only communication between the defendant and the victim, but also for any programs containing "child pornography". Further, Detective Phillips testified that he was specifically looking for child pornography in addition to evidence of contacts between

defendant and D.C.

Detective Casady and Detective Phillips believed that they were authorized to search for child pornography because (1) the victim had admitted that there had been sexual contact between himself and the defendant on more than one occasion, (2) police had observed the XY magazine in defendant's residence, (3) Detective Casady had been taught in her training that it is common to find child pornography in the possession of child predators, and (4) the warrant authorized the seizure of any and all electronic and internal media and data stored within the computer and cell phone.

While evidence obtained as a result of a defective search warrant is generally inadmissible, Mapp v. Ohio, 367 U.S. 643 (1961), there is an exception for evidence found by officers relying in objective good faith on a defective search warrant. United States v. Leon, 468 U.S. 897, 920-21 (1984) (establishing the good faith exception). However, four circumstances exist in which the Leon good faith exception does not apply: (1) the judge issuing the warrant was misled by statements made by the affiant that were false or made in reckless disregard for the truth; (2) the issuing judge wholly abandoned his or her judicial role; (3) the affidavit in support of the warrant is so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable, or (4) the warrant is so

facially deficient that the executing officers cannot reasonably presume it to be valid. United States v. Taylor, 119 F.3d 625, 629 (8th Cir. 1997) (citing Leon, 468 U.S. at 923). A reviewing court can apply the Leon good faith exception and evaluate the reasonableness of an officer's reliance on a warrant without first resolving the Fourth Amendment issue of whether the search warrant lacked probable cause. United States v. Guzman, -- F.3d --, 2007 WL 3241180 (8th Cir., November 5, 2007), citing United States v. Weeks, 160 F.3d 1210, 1212 (8th Cir. 1998). Accordingly, I will assume without deciding that the affidavit supporting the search warrant lacked probable cause to search for "any and all" media and data contained within the computer.

"Suppression of evidence obtained pursuant to a warrant should be ordered only on a case-by-case basis and only in those unusual cases in which exclusion will further the purposes of the exclusionary rule." United States v. Leon, 468 U.S. at 918. The Eighth Circuit recently addressed the good faith exception to the exclusionary rule in the context of a computer search in United States v. Grant, 490 F.3d 627, 632-33 (8th Cir. 2007). "Under the Leon good-faith exception, disputed evidence will be admitted if it was objectively reasonable for the officer executing a search warrant to have relied in good faith on the judge's determination that there was probable cause to issue the warrant. In assessing whether the officer relied in good faith on the

validity of a warrant, we consider the totality of the circumstances, including any information known to the officer but not included in the affidavit and we confine our inquiry to the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal despite the [issuing judge's] authorization". Id. at 632, citations omitted.

In this case, there is ample evidence of the officers' good faith reliance on the warrant. The officers did not seize a magazine displaying a young boy wearing only boxers, they did not seize police radios or scanners, they did not seize a camera. All of those items were left behind because the officers did not believe they were within the scope of the search warrant. This is evidence of the officers' knowledge of their obligation not to engage in a general search and to remain within the scope of the warrant.

Detective Casady knew that her department had obtained about fifteen warrants seeking computer media, she knew that all of those warrants had contained language similar to the warrant in this case, she knew that none of them had been challenged in court. She had at least three other officers and an assistant prosecutor review the affidavit before it was presented to a judge. Detective Casady had been trained that child predators commonly possess child pornography, and she knew that an XY

magazine had been found in defendant's residence. Detective Casady's request to RCFL, which instructed the lab to search for child pornography, was based on her believe that the warrant authorized such a search because it authorized the seizure of any and all media and data on the computer.

Detective Phillips, who was assigned to do the preview of the computer media, stated under oath that he believed the warrant authorized him to look at anything on the computer. He also testified that he believed the search for child pornography was authorized because child pornography and child enticement "go hand in hand."

Finally, forensic examiner Richard Gatewood reviewed the warrant before conducting his search to make sure it covered the service request. He believed his thorough search was authorized by the warrant because it authorized the search and seizure of "any and all electronic media".

In addition to this evidence of good faith on the part of the police, there is no evidence of any of the factor precluding the good faith exception.

There is no allegation that the affidavit contains a false statement or material omission.

There is no evidence that the issuing judge abandoned his judicial role in any way. The judge read the affidavit and application, and he changed an incorrect date on the warrant

indicating that he had read it carefully.

The affidavit clearly establishes probable cause that evidence of a crime would be found in defendant's computer and cell phone, as it is alleged that defendant had daily contact with his victim through his computer and his cell phone.

Finally, the presumption by the officers that the warrant authorized the search performed was objectively reasonable. The Lee's Summit police department had issued many similar warrants in the past with no adverse court holdings on any of them. In addition, their training taught them that child predators commonly possess child pornography.

Based on all of the above, I find that even if the warrant was defective in that it lacked the particularly requirement by authorizing the seizure of "any and all" media and data, the good-faith exception to the exclusionary rule applies and the evidence seized should therefore not be suppressed.

IV. ILLEGAL EXECUTION OF THE SEARCH WARRANT

Defendant next argues that the search warrant was illegally executed because the police did not obtain further permission from a judge to search "relevant computer files intermingled with irrelevant computer files". In light of the above discussion (i.e., that the police reasonably believed that the warrant authorized the search of all of the computer's files), this argument is without merit. However, several issues merit further

discussion.

First, I note that the case relied on heavily by the defendant, United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001), is clearly distinguishable. In that case, the defendant's computer was being searched for evidence of illegal drug sales. When the officer came across what he believed to be child pornography, he immediately ceased his search of the computer and submitted an affidavit for a new search warrant specifically authorizing a search for evidence of possession of child pornography. That was because the officer did not believe that his search warrant authorized the seizure of child pornography, and it was his intent to obtain a warrant which would allow him specifically to search for and seize child pornography. However, in this case, the officers reasonably believed that the warrant that had already been issued authorized the seizure of child pornography in addition to evidence of child sexual exploitation.

Second, the intent of the police to search for child pornography despite whether the affidavit made any mention of child pornography, is not a determining factor for suppression. That is, the intent of the police does not govern; rather what governs is the extent of the search and whether it exceeded the scope of the search that was authorized by the warrant.

It is well settled that the subjective intent of the police does not invalidate an otherwise lawful stop or search. For

example, the subjective belief of an officer that there might be illegal drugs in a vehicle does not invalidate a stop based on a minor traffic offense. United States v. Martinez, 358 F.3d 1005, 1009 (8th Cir. 2004). Thus, "a traffic-violation arrest . . . would not be rendered invalid by the fact that it was a 'mere pretext for a narcotics search.'" Whren v. United States, 517 U.S. 806, 812-13 (1996) (quoting United States v. Robinson, 414 U.S. 218, 221 n. 1 (1973)).

Therefore, the detectives' hope to find child pornography on defendant's computer would not invalidate the search when the warrant authorized the search of "any and all" media and data on the computer for evidence of child sex crimes. The search would be no greater, i.e., no more intrusive, because of the detectives' hope to find child pornography as well as evidence of child sex crimes.

In addition, the evidence establishes that in order to find the instant messages and chat room logs being sought, police would need to look through graphics files. Police may look in any place where the evidence sought may be found. This argument -- that the police should have restricted their search to text files -- has been rejected by other courts, and I find that reasoning persuasive. For example, in United States v. Kearns, 2006 WL 2668544 (N.D. Ga. 2006), the court upheld the seizure of child pornography images from computer media obtained with a

search warrant that authorized a search for evidence of financial, accounting, and real estate fraud. The court declined to adopt the argument that the search methodology should have been limited to apparent text files. The court noted that the reasonableness of the agent's search of the computer media under the Fourth Amendment did not turn on whether the search was the most technically advanced. The court also noted that files can be mis-designated, or intentionally concealed, such that a cursory view of all files may be necessary. Id. at *5-*7. The court recognized that the search of Kearns's computer media was going to have to be all-encompassing, and the court upheld the finding of the child pornography images as having been in plain view during the continuing, methodical, authorized search of the media for the evidence set out in the warrant.

> [A] "warrant must enable the executing officer to ascertain and identify with reasonable certainty those items that the magistrate has authorized him to seize." See United States v. George, 975 F.2d 72, 75 (2nd Cir. 1992). In some cases, however, it is not immediately apparent whether an item is within the scope of the search warrant; and, in such cases, an agent must briefly examine the item to determine whether it is one that he is authorized to seize. United States v. Slocum, 708 F.2d 587, 604 (11th Cir. 1983).
>
> . . . "[T]he search 'may be as extensive as reasonably required to locate and seize items described in the warrant.' The reasonableness of the search depends upon the complexity of the crime being investigated and the difficulty involved in determining whether certain documents evidence fraud." United States v. Sawyer, 799 F.2d 1494, 1509 (11th Cir. 1986) (internal citations omitted). Therefore, "in some instances, searching officers must be able to examine nearly every document possessed by a suspected criminal, if only to determine whether the

documents contain evidence of criminal activity." United States v. Le, 173 F.3d 1258, 1276 (10th Cir. 1999).

Id. at *5.

Finally, while the issue has not been squarely addressed in the Eighth Circuit, courts in other circuits are essentially in agreement that a warrant "need not specify how the computers will be searched." United States v. Vilar, 2007 WL 1075041, *37 (S.D.N.Y. April 4, 2007) (reviewing cases on the issue and concluding that the "vast majority" have come to this conclusion). This is in accordance with the Supreme Court's statement that "it is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search". Dalia v. United States, 441 U.S. 238, 257 (1979). The rule, however, does not give investigators "free reign," as they are always subject to the requirement of reasonableness. Vilar at *37. But it recognizes that "courts are ill-equipped" to get into the business of telling investigators what to do. Id. at *38.

Significantly, the Vilar court addressed the issue, raised in this case by both defendant and the government, of the sufficiency of a "key-word" search: "[I]t seems manifestly obvious that any requirement that a computer search be confined by a key-word search protocol would inevitably immunize criminals. Such a simplistic search paradigm would of necessity leave out any encoded documents, or any documents that used

acronyms or other abbreviations in place of the 'key words.' Moreover, there may be numerous 'documents' that are not word-searchable and would therefore not be discovered in a search restricted to key-word inquiries." Vilar at *38.

Viewing defendant's computer as the "vessel" to be searched, once the officers were "in" that vessel, the analysis of what was done thereafter is an analysis of the method or manner of the search, and not one of whether the search was justified. Applying the reasoning of Vilar, the manner in which defendant's computer was searched passes constitutional muster. Opening the individual files on defendant's computer was not an event subject to traditional probable cause analysis, but rather a method, subject simply to the requirement of "reasonableness," with great deference given to the expertise of the officers.

V. CONCLUSION

Based on the above-stated findings of fact and the law as discussed in sections III and IV, I find that regardless of whether the particularly requirement of the Fourth Amendment was met with regard to the items to be seized, the good-faith exception to the exclusionary rule applies. Therefore, it is

RECOMMENDED that the court, after making an independent review of the record and the applicable law, enter an order denying defendant's motion to suppress evidence.

Counsel are advised that, pursuant to 28 U.S.C. § 636(b)(1), each has ten days from the date of this report and recommendation to file and serve specific objections.

/s/ Robert E. Larsen
ROBERT E. LARSEN
United States Magistrate Judge

Kansas City, Missouri
December 3, 2007